

KELLEY DRYE & WARREN LLP

A LIMITED LIABILITY PARTNERSHIP

WASHINGTON HARBOUR, SUITE 400

3050 K STREET, NW

WASHINGTON, D.C. 20007-5108

NEW YORK, NY

CHICAGO, IL

STAMFORD, CT

PARSIPPANY, NJ

BRUSSELS, BELGIUM

AFFILIATE OFFICES

MUMBAI, INDIA

FACSIMILE

(202) 342-8451

www.kelleydrye.com

(202) 342-8400

DIRECT LINE: (202) 342-8640

EMAIL: dcrock@kelleydrye.com

February 25, 2009

VIA ECFS

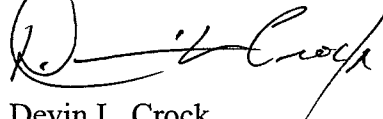
Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

Re: Annual Customer Proprietary Network Information Compliance
Certification; EB Docket No. 06-36

Dear Ms. Dortch:

Pursuant to 47 C.F.R. § 64.2009(e), SNiP LiNK, LLC hereby provides its Annual Customer Proprietary Network Information Compliance Certification. Please feel free to contact me if you have any questions regarding this filing.

Sincerely,



Devin L. Crock

Annual Customer Proprietary Network Information Certification
Pursuant to 47 C.F.R. § 64.2009(e)
EB Docket No. 06-36
February 2009

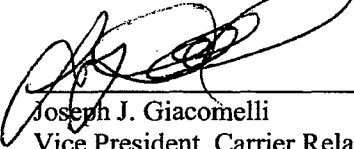
Name of Company: SNiP LiNK, LLC
Form 499 Filer ID: 820377
Name of Signatory: Joseph J. Giacomelli
Title of Signatory: Vice President, Carrier Relations

I, Joseph J. Giacomelli, certify that I am an officer of SNiP LiNK, LLC ("SNiP LiNK"), and acting as an agent of SNiP LiNK, that I have personal knowledge that SNiP LiNK has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how SNiP LiNK's procedures ensure the company is in compliance with the requirements set forth in sections 64.2001 *et seq.* of the Commission's rules.

SNiP LiNK has not taken any actions (instituted proceedings or filed petitions at either state commissions, courts, or at the FCC) against data brokers in the past year. SNiP LiNK has no information outside of Commission Docket No. 96-115, or that is not otherwise publicly available (*e.g.*, through news media), regarding the processes pretexters are using to attempt to access CPNI.

SNiP LiNK has not received any customer complaints in the past year concerning the unauthorized release of CPNI.



Joseph J. Giacomelli
Vice President, Carrier Relations
SNiP LiNK, LLC

Date: 2/25/09

Customer Proprietary Network Information Certification Attachment A

SNiP LiNK has established practices and procedures adequate to ensure compliance with Section 222 of the Communications Act of 1934, as amended, and the Federal Communications Commission's ("FCC") rules pertaining to customer proprietary network information ("CPNI") set forth in sections 64.2001 – 64.2011 of the Commission's rules. This attachment summarizes those practices and procedures.

Safeguarding against pretexting

- SNiP LiNK takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI, including the authentication of customers prior to disclosing CPNI based on customer-initiated contacts. SNiP LiNK is committed to notify the FCC of any novel or new methods of pretexting it discovers and of any actions it takes against pretexters and data brokers.

Training and discipline

- SNiP LiNK trains its supervisory and non-supervisory personnel in an effort to ensure that its employees, in accordance with FCC regulations: (a) understand what CPNI is, (b) join in and carry-out SNiP LiNK's obligation to protect CPNI, (c) understand when they are and when they are not authorized to use or disclose CPNI, (d) obtain customers' informed consent as required with respect to its use for marketing purposes, and (e) keep records regarding receipt of such consent, customer complaints regarding CPNI and the use of CPNI for marketing campaigns.
- SNiP LiNK employees are required to review SNiP LiNK's CPNI practices and procedures.
- SNiP LiNK requires all outside Dealers and Agents to acknowledge and certify that they may only use CPNI for the purpose for which that information has been provided.
- SNiP LiNK has an express disciplinary process in place for violation of the SNiP LiNK's CPNI practices and procedures. The careless or intentional failure to comply with these practices and procedures may result in disciplinary action, up to and including discharge.

SNiP LiNK's use of CPNI

- SNiP LiNK may use CPNI for the following purposes:
 - To initiate, render, maintain, repair, bill and collect for services;
 - To protect its property rights; or to protect its subscribers or other carriers from fraudulent, abusive, or the unlawful use of, or subscription to, such services;
 - To provide inbound telemarketing, referral or administrative services to the customer during a customer initiated call and with the customer's informed consent.
 - To market additional services to customers that are within the same categories of service to which the customer already subscribes;
 - To market services formerly known as adjunct-to-basic services; and
 - To market additional services to customers *with the receipt of informed consent via the use of opt-in or out-out, as applicable.*
- SNiP LiNK does not disclose or permit access to CPNI to track customers that call competing service providers.

- SNiP LiNK discloses and permits access to CPNI where required by law (e.g., under a lawfully issued subpoena).

Customer approval and informed consent

- SNiP LiNK has implemented a system to obtain approval and informed consent from its customers prior to the use of CPNI for marketing purposes. This system also allows for the status of a customer's CPNI approval to be clearly established prior to the use of CPNI.
 - Prior to any solicitation for customer approval, SNiP LiNK will notify customers of their right to restrict the use of, disclosure of, and access to their CPNI.
 - SNiP LiNK will use opt-in approval for any instance in which SNiP LiNK must obtain customer approval prior to using, disclosing, or permitting access to CPNI.
 - A customer's approval or disapproval remains in effect until the customer revokes or limits such approval or disapproval.
 - Records of approvals are maintained for at least one year.
 - SNiP LiNK will provide individual notice to customers when soliciting approval to use, disclose, or permit access to CPNI.
 - The content of SNiP LiNK's CPNI notices comply with FCC rule 64.2008(c).

Opt-in

- SNiP LiNK does not share, disclose, or otherwise provide CPNI to third parties for marketing purposes.

One time use

- After authentication, SNiP LiNK uses oral notice to obtain limited, one-time approval for use of CPNI for the duration of a call. The contents of such notice comports with FCC rule 64.2008(f).

Additional safeguards

- SNiP LiNK will maintain for at least one year records of all marketing campaigns that use its customers' CPNI, including a description of each campaign and the CPNI used, the products offered as part of the campaign, and instances where CPNI was disclosed to third parties or where third parties were allowed access to CPNI. Such campaigns are subject to a supervisory approval and compliance review process, the records of which also are maintained for a minimum of one year.
- SNiP LiNK has established a supervisory review process designed to ensure compliance with the FCC's CPNI rules.
- Online access to CPNI is only available to SNiP LiNK's business customers. SNiP LiNK requires its customers to provide an alphanumeric password prior to disclosing CPNI online.
- Before disclosing CPNI over the telephone, SNiP LiNK calls the customer back at the telephone number of record to authenticate the customer.
- SNiP LiNK notifies customers immediately of any account changes, including address of record, authentication, online account and password related changes.

- SNiP LiNK may negotiate alternative authentication procedures for services that SNiP LiNK provides to business customers that have both a dedicated account representative and a contract that specifically addresses SNiP LiNK's protection of CPNI.
- In the event of a breach of CPNI, SNiP LiNK will notify law enforcement as soon as practicable and no later than seven (7) business days from discovering the breach. Customers will be notified after the seven (7) day period, unless the relevant investigatory party directs SNiP LiNK to delay notification, or SNiP LiNK and the investigatory party agree to an earlier notification. SNiP LiNK will maintain a record of all CPNI security breaches, including a description of the breach and the CPNI involved, along with notifications sent to law enforcement and affected customers.
- When SNiP LiNK discloses to or provides independent contractors or joint venture partners with access to CPNI, it does so pursuant to confidentiality agreements that (a) require the independent contractor/joint venture partner to use CPNI only for the purpose it has been provided, (b) prohibit independent contractor/joint venture partners disclosure of such CPNI except under force of law, and (c) require the independent contractor/joint venture partner to have appropriate protections in place to ensure the ongoing confidentiality of the CPNI.